

IT'S DATA PRIVACY WEEK

Here is why your business should care



What is Data Privacy?

Data privacy involves the protection of data with regards to its collection, usage, and distribution. "Data", in this case, typically refers to any information that could personally identify someone, such as their name, address, phone number, social security number, credit card information, or their username and password.



The Growing Concern

46% of consumers feel they've lost control over their own data. (Salesforce)

53%

53% of companies have more than 1,000 sensitive files open to every employee. (Varonis)

Why Businesses Should Take Privacy Seriously

92%

92% of consumers say companies must be proactive about data protection. (PwC)

48%

48% of consumers have stopped buying from a company over privacy concerns. (Tableau)

64%

64% of Americans would blame the company, not the hacker, for the loss of personal data. (RSA)

\$3.92M

The average data breach costs \$3.92 million. (IBM)

279 DAYS

The average time to detect and contain a breach is 279 days. (IBM)

The Business ROI of Strong Data Privacy

97%

97% of companies have seen benefits, like a competitive advantage or investor appeal, from investing in privacy. (Cisco)

84%

84% of consumers are more loyal to companies that have strong security controls. (Salesforce)

70%

More than 70% of organizations say they receive significant business benefits from privacy, including operational efficiency, agility and innovation. (Cisco)

DATA PRIVACY WEEK

5 WAYS TO STRENGTHEN DATA PRIVACY AT WORK

1

Use a VPN for work-related tasks

AVPN (VirtualPrivateNetwork) allows you to create a secure connection to another network over the Internet that obscures your online identity, even on public Wi-Fi networks, so you can browse the internet safely and anonymously.

2

Don't log onto unsecure networks

Using public Wi-Fi when working, such as in a coffee shop, can be risky, as hackers can position themselves between you and the connection point and launch a malware attack.

3

Watch out for scams

It's easy to think that cyber criminals would never target you, but just remember that all staff have access to valuable data that attackers are just waiting to exploit through attacks like phishing.

4

Be aware of eavesdropping

With many meetings taking place over conference calls these days, it's important to make sure sensitive info isn't shared in public places, as well as to keep devices physically secure.

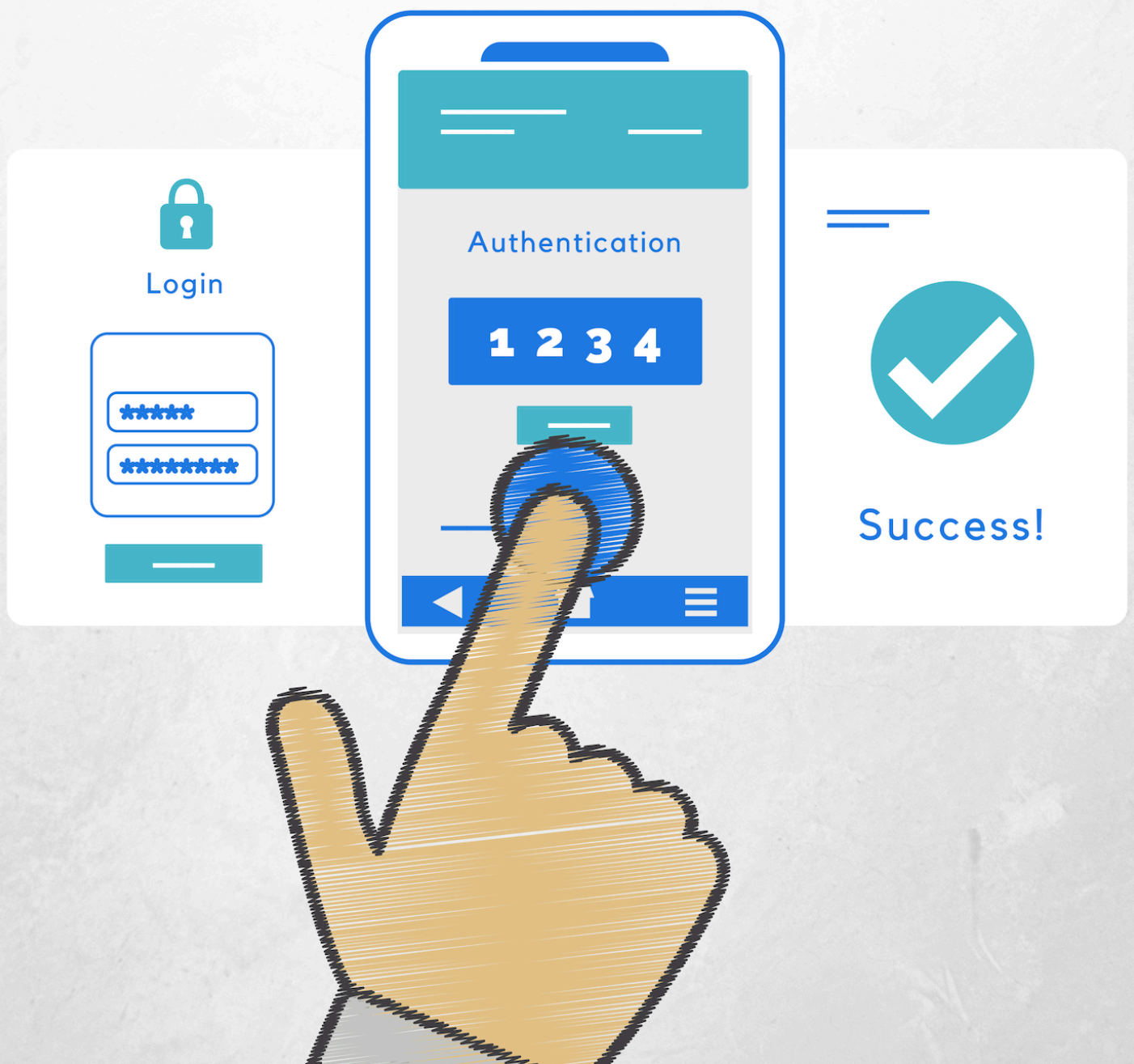
5

Limit backups of devices

While backups are necessary for data recovery, each backup results in additional data proliferation. Ensure that staff are instructed on data privacy and security best-practices through regular security awareness training and up-to-date policies.

Avoid being an 'easy-picking' for
cyber criminals. Enable...

Two-Factor Authentication



Data *Protection* Is In Your Hands

An illustration of a right hand, rendered in a light tan color with simple black outlines for the fingers and wrist. The hand is positioned as if it is about to touch or hold the word "Protection" in the title. The background is a solid dark blue.

**Think twice before
sharing information**

Emailing sensitive data?



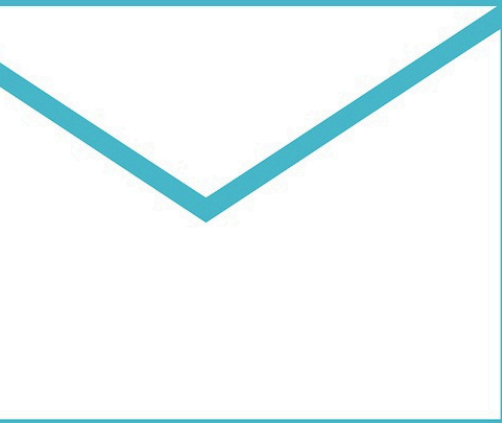
Make sure you haven't
entered the **wrong** recipient

To: XXX

Cc: XXX

Bcc: XXX

Emailing Sensitive Data?



To: XXXX

Cc: XXXX

Bcc: XXXX

Always double check that you've
entered the **correct recipient**.

Don't make life easy for cyber criminals.

On the move?

Please be careful
with **physical data** when
taken off-site.



Handling **Data**? Think **Protection**.

Leaving your desk?



Keep data secured by locking your computer and devices **when not in use.**

Don't make life easy for cyber criminals.

How strong is your Password?

Weak passwords are easy to crack.
Keep things safe by making sure you...



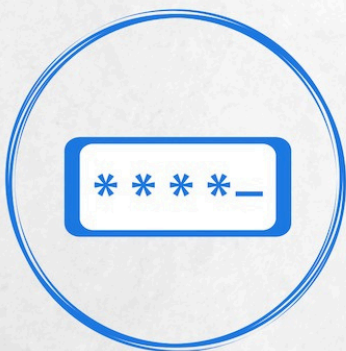
Keep it long and complicated



Use both upper and lower case letters



Avoid guessable info (e.g., D.O.B)



Implement two-factor authentication



Change your password regularly



Never share your password

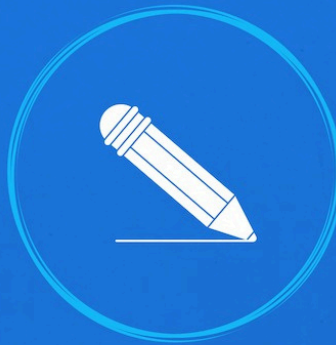
Don't make life easy for cyber criminals.

Don't fall for the PHISHING bait!

Be suspicious of...



Hyperlinks to fake
websites



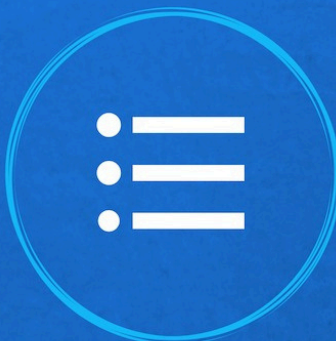
Unofficial "From"
addresses



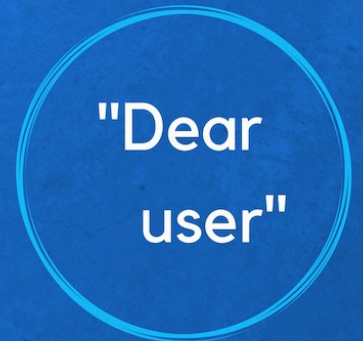
"Urgent" requests
or threats



Emails containing
attachments



Requests for
sensitive information



Generic subject lines
and intro messages

Don't make life easy for cyber criminals.

Handling **Data**? Think **Protection**.



Think

before leaving sensitive
documents **unattended**.

All of the information
you work with has

Value.



Data Privacy Week

Email Prospecting Template

Subject:

Turn Your Employees into Your Strongest Security Asset

Email Body:

Hi [First Name],

As Data Privacy Week 2025 approaches, this is the perfect time to strengthen how your workforce handles sensitive company data.

Looking to make data security more manageable this year? We've got you covered!

We're offering a 14-day free trial of our enhanced Human Risk Management (HRM) service that transforms your employees into your strongest security asset.





Here is how our managed HRM service can strengthen your business's data privacy:

- Engage employees with bite-sized training on safe data handling and privacy practices.
- Automate essential policies for data privacy compliance without the hassle.
- Monitor risks in real-time with ongoing dark web breach detection.
- Boost resilience through phishing simulations that teach employees to spot threats.

Getting started is quick, hassle-free, and requires no commitment.

We would love to schedule a call with you so that we can discuss how our HRM service can help your business stay compliant and protect your data.

Sincerely,

Post 1: Why Data Privacy Matters

Data Privacy: Protect What's Yours!

In today's digital age, protecting your data is more important than ever. During Data Privacy Week, take the opportunity to review your data privacy practices and secure your sensitive information.

- ✓ Use strong passwords
- ✓ Enable multi-factor authentication (MFA)
- ✓ Be cautious of phishing scams

Ready to take the next step?

👉 Start today with our **14-day free trial** and improve your security awareness training.

#DataPrivacy #CyberSecurity #ProtectYourData #DataPrivacyWeek #SecurityAwareness

Post 2: Human Risk Management

Mitigate Human Risk with Security Awareness Training

Did you know that human error is one of the leading causes of data breaches? Even with the best technology, awareness training is key to minimizing risk.

🌐 Protect your organization by educating your team on data privacy and security best practices.

Want to get started?

👉 Read more on how to reduce human risk and protect your data in our latest blog post.

#HumanRisk #DataSecurity #SecurityAwareness #CybersecurityTraining #DataPrivacyWeek

Post 3: Data Privacy Best Practices

5 Tips to Protect Your Data

1. Use complex passwords
2. Enable multi-factor authentication (MFA)
3. Regularly update software
4. Encrypt sensitive data
5. Stay aware of phishing attacks

Don't wait—implement these best practices now to protect your data.

Need help getting started? Try our 14-day free trial.

#DataPrivacyBestPractices #CyberSecurity #SecureYourData #DataPrivacyWeek
#ProtectYourData